# The Topology of Quantum Algorithms

Jamie Vicary
jamie.vicary@cs.ox.ac.uk

Centre for Quantum Technologies, University of Singapore
and Department of Computer Science, University of Oxford

September 18, 2012

**Abstract**

We use a topological formalism to examine the Deutsch-Jozsa, hidden subgroup and Grover algorithms. This reveals important structures hidden by conventional algebraic presentations, and allows short and visual proofs of correctness via local topological operations. The resulting transparency makes generalizations of these algorithms clear, which gives rise to simpler descriptions of generalized Deutsch-Jozsa and hidden subgroup algorithms already in the literature, and a new generalization of Grover's algorithm.

## 1 Overview

### 1.1 Introduction

Important quantum procedures often seem mysterious because of the low-level way in which they are presented. A direct description of the required state preparations, unitary operators and projective measurements in terms of matrices of complex numbers gives exactly the required information to actually implement a particular protocol — but almost no information about why it should work.

One reason for this is that quantum information has a *topological* nature. The overall effect of a composite of quantum operations depends not so much on the order of composition, as on the topological flows of information that this induces, as demonstrated in striking fashion by Abramsky, Coecke et al [1, 2, 6, 7, 8, 9, 10, 11, 12]. Their high-level techniques de-emphasize the matrices of complex numbers used in conventional presentations of many important quantum procedures, replacing them with topological primitives that give a satisfying explanation for why these procedures work. Extended by the author to cover the flow of classical information [24], this body of work gives a mature set of tools for analyzing a wide range of quantum procedures, especially those which make use of Bell-type entanglement or complementary observables.

However, quantum *algorithms*, such as the Deutsch-Jozsa, hidden subgroup or Grover protocols, have so far not been analyzed as part of this research programme. These can be usefully distinguished from quantum *procedures* such as quantum teleportation, dense coding and key exchange, which bring about a certain physical effect rather than compute a particular quantity. Features of these algorithms that make them hard to

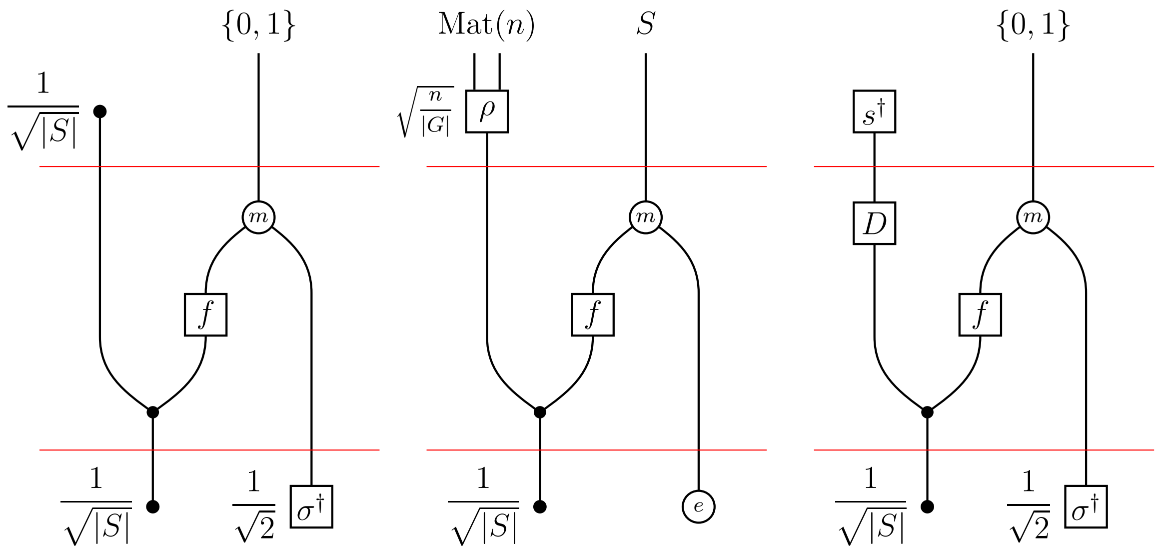
model using the topological formalism include the use of an oracle and the reliance on group representation theory, as well as the nondeterminism of the hidden subgroup and Grover algorithms.

## 1.2 Topological algorithms

This paper overcomes these difficulties by giving a topological characterization of the structure of the quantum oracle, as well as the necessary results from group theory on which these algorithms implicitly rely. We obtain topological accounts of the Deutsch-Jozsa, hidden subgroup and (in a restricted form) Grover algorithms, with visual proofs of correctness that are significantly simpler than standard treatments, and which carry more insight. Throughout, our focus is on the structure of the algorithms rather than on efficiency.

Another key benefit of the topological perspective is that certain generalizations of the algorithms become immediately obvious, with proofs of correctness almost identical to that for the standard versions of the algorithms. For the Deutsch-Jozsa and hidden subgroup algorithms, these generalizations are already in the literature. In these cases, our techniques offer simpler proofs, and new insight into the structures involved. In the case of Grover's algorithm, the generalization appears to be new.

The topological forms of the Deutsch-Jozsa, hidden subgroup and Grover algorithms that we develop are summarized here:




**Deutsch-Jozsa** **Hidden subgroup** **Grover**

The horizontal lines separate the state preparation phase at the bottom of each diagram, the unitary dynamics phase in the centre, and the projective measurement phase at the top. Section 3 introduces the notation used to construct these diagrams. We explore these algorithms in Sections 4, 5 and 6 respectively.

There are strong similarities between these algorithms, which are already apparent in the conventional presentations. Common features include the two systems on which the algorithm operates, the initial state for the first system, the unitary oracle dynamics, and the final measurement taking place only on the first system. However, perhaps surprisingly, there seems to be no interesting general procedure for which any two of these are special cases.

Certain features of these algorithms are often not presented clearly in the literature, but are made obvious using our formalism. For example, it is sometimes claimed that the Deutsch-Jozsa algorithm is an instance of the hidden subgroup algorithm [17, 19], perhaps because of the broad similarities between the algorithms as mentioned above. However, the specific forms of the algorithms, and in particular the topological proofs of correctness we will present, are quite different. Also, for all three of these algorithms, it is often suggested that an additional measurement on the *second* system is required after the unitary dynamics phase. This is not the case, as the topological proofs make clear.

Our proofs of correctness proceed by performing local topological rewrites of the diagrams defining the algorithms. These rewrites are topological encodings of results in the linear algebra of finite sets and finite groups, developed in Section 3 and in the Appendix. The resulting proofs are short, clear and structurally informative, allowing the high-level topological arguments to proceed separately from the group theoretical analysis.


**Acknowledgements**

This project grew out of discussions with Bob Coecke. I am grateful to John Baez, Bob Coecke, Brendan Fong and William Zeng for useful comments. Diagrams have been produced using the package `TikZ`. This work was supported by funding from the Centre for Quantum Technologies at the National University of Singapore, as a part of the *Quantum Nanoscience* project.


# 2 The traditional Deutsch-Jozsa algorithm

## 2.1 The setup

We begin by outlining the usual presentation of the Deutsch-Jozsa algorithm, as can be found in standard reference texts such as [19]. As we proceed we highlight certain unclear or mysterious features of the algorithm, which will be resolved by our new graphical presentation in Section 4.

The conventional Deutsch-Jozsa algorithm involves a function

$$\{0,1\}^N \xrightarrow{f} \{0,1\}, \tag{1}$$

where $\{0,1\}$ is the group of integers under addition modulo 2, and $\{0,1\}^N$ is the $N$-fold cartesian product of this for some natural number $N$. This function is promised to have one of two properties: it is either *constant*, meaning that it takes the same value on every element of $S$; or *balanced*, meaning that it takes each possible value on exactly half of the elements of $S$. This gives us a first question:

*Why should "constant" or "balanced" be important properties?*

They seem rather mysterious, and it would be good to have some high-level understanding of why they arise.

We then construct a unitary operator

$$(\mathbb{C}^2)^N \otimes \mathbb{C}^2 \xrightarrow{U_f} (\mathbb{C}^2)^N \otimes \mathbb{C}^2 \tag{2}$$

from our function $f$, which is defined to act in the following way:

$$|k\rangle \otimes |b\rangle \overset{U_f}{\longmapsto} |k\rangle \otimes |b \oplus f(k)\rangle \tag{3}$$

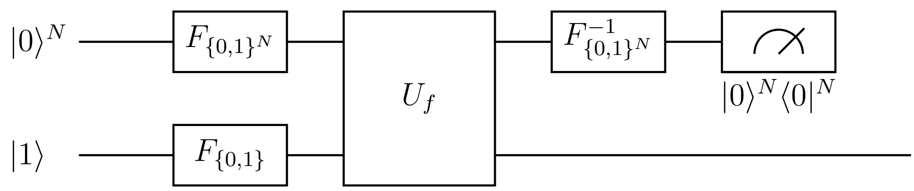
Here $k$ is an element of $\{0,1\}^N$, and $b$ is an element of $\{0,1\}$. The symbol $\oplus$ represents addition modulo 2, which is the group structure on $\{0,1\}$. This poses another question:

*Does the group structure on* $\{0,1\}^N$ *play an essential role?*

It has not been relevant so far, in the definitions of constant or balanced function or in the definition of $U_f$.

## 2.2 The procedure

We use $U_f$ to build the following quantum circuit.




(4)

We read this from left to right, as is conventional for quantum circuit diagrams. We begin by preparing $N$ qubits in the state $|0\rangle$, and a single qubit in the state $|1\rangle$. We then apply the unitary operators $F_{\{0,1\}^N}$ and $F_{\{0,1\}}$, representing the Fourier transform operations on the groups $\{0,1\}^N$ and $\{0,1\}$ respectively. The operator $U_f$ is then applied, followed by an inverse Fourier transform $F^{-1}_{\{0,1\}^N}$ on the upper family of $N$ qubits, and a projective measurement onto the state $|0\rangle^N$. The lower qubit plays no role after the application of the unitary $U_f$.

It might seem that this provides an answer to Question 2.1 above, since the group structure on $\{0,1\}^N$ is used to construct the Fourier transform operator $F_{\{0,1\}^N}$. However, we only apply this Fourier transform operator to the element $|0\rangle^N$, which represents the identity element of the group. On this element, the Fourier transform acts as follows, creating an even superposition of the group elements:

$$F_{\{0,1\}^N}(|0\rangle^N) = \frac{1}{\sqrt{2^n}} \sum_{k\in\{0,1\}^N} |k\rangle \tag{5}$$

But this superposition is *independent* of the group structure, since the Fourier transform on any abelian group gives this result for some group element. The application of $F^{-1}_{\{0,1\}^N}$ at the end of the protocol is insensitive to the group structure for the same reason, since it is followed by a projective measurement onto the state $|0\rangle$, and hence its sole function is to allow an effective projective measurement onto the same superposition state (5).

Further questions are also raised by the quantum circuit given above.

*Why should we prepare the upper qubits in the state* $|0\rangle^N$*?*

A partial answer to this question is given by the reasoning above: by the action of the Fourier transform, it allows us to access an even superposition of every element of $\{0,1\}^N$, and hence, in some sense, probe our function $f$ on "every input simultaneously". But this is a vague notion: for what high-level reason should it enable the protocol to succeed? We can ask a similar question for the lower qubit:

*Why should we prepare the lower qubit in the state* $|1\rangle$*?*

The Fourier transform $F_{\{0,1\}}$ acts on this state to produce the superposition $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Why should this be the correct state to feed into the operator $U_f$?

### 2.3 The measurement

The last step of the algorithm is to perform a projective measurement on the upper family of qubits onto the state $|0\rangle^N$. As discussed, given that this follows an application of the inverse Fourier transform $F^{-1}_{\{0,1\}^N}$, the overall effect is to measure the qubits in the state (5). If the projective measurement is successful, then we can conclude with certainty that our original function $f$ is balanced. If the measurement fails, then we can conclude with certainty that $f$ is constant. Confusingly, in some presentations, a measurement onto the lower family of qubits is also involved.

Some further questions naturally raise themselves here.

*Why should we measure the upper qubits in the state $|0\rangle^N$?*

*Why should we expect the measurement to succeed or fail exactly when the original function was constant or balanced?*

*Should measurement on the second family of qubits play a role?*

A high-level understanding of the Deutsch-Jozsa algorithm will provide good answers to all these questions, as we see in the next section.

More ambitiously, we could also ask the following final question.

*Can this algorithm be generalized?*

This traditional presentation gives no indication as to whether this is the case. In fact, there is a broad class of possible generalizations, and the topological perspective we describe makes them almost obvious.

## 3 Topological algebra

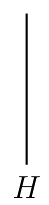
### 3.1 Introduction

In this section we present a topological notation for linear algebra, and show how it gives a powerful way to display various properties of finite groups and finite sets. Built on early work of Penrose [20], these techniques have now found wide use in quantum foundations and quantum information [3, 6, 16]. A mathematical foundation for the notation is given by category theory [15, 22], but this will remain entirely beneath the surface in this paper.

We begin by defining the notation, then demonstrate how we can use it to represent theorems about finite sets and finite groups in a topological way. These will form the heart of our topological proofs of the Deutsch-Jozsa, hidden subgroup and Grover algorithms.

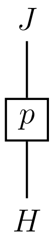
### 3.2 Linear algebra

In the topological notation, diagrams represent linear maps between finite-dimensional Hilbert spaces. A vertically-oriented wire represents the identity map on a finite-dimensional Hilbert space, which we will often label with its name:




(6)

Nontrivial linear maps are represented by boxes, or sometimes simply by a vertex, with its domain represented by the input wires at the bottom, and its codomain represented by output wires at the top. So we draw the following diagram to represent a linear map of type $H \xrightarrow{p} J$:

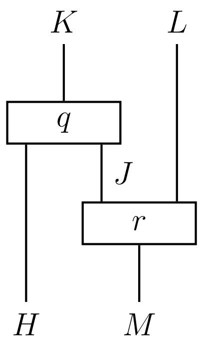



(7)

Horizontal juxtaposition of diagrams represents tensor product of linear maps, and vertical juxtaposition represents composition of linear maps. So, for example, given maps $H \otimes J \xrightarrow{q} K$ and $M \xrightarrow{r} J \otimes L$


(8)

we represent the composite $(q \otimes \mathrm{id}_L) \circ (\mathrm{id}_H \otimes r)$ with the following diagram:




(9)

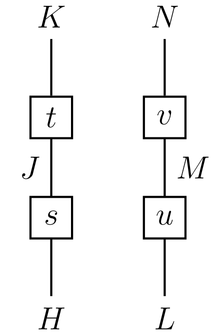
The identity on the 1-dimensional Hilbert space $\mathbb{C}$ is represented as the empty diagram:

(10)

Juxtaposing this with any diagram leaves the diagram unchanged, which makes sense, because up to isomorphism it is the unit for the tensor product operation.

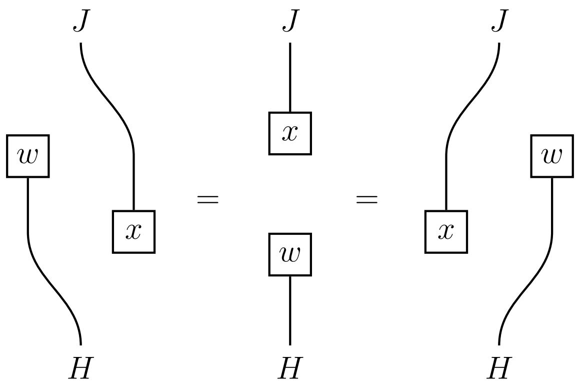
Nontrivial algebraic interactions between the tensor product and composition of linear maps are made transparent by the formalism. In particular, for a family of maps $H \xrightarrow{s} J$, $J \xrightarrow{t} K$, $L \xrightarrow{u} M$ and $M \xrightarrow{v} N$, the equal algebraic composites $(t \otimes v) \circ (s \otimes u)$ and

$(t \circ s) \otimes (v \circ u)$ have the same graphical representation:




(11)

The formalism also allows us to change the relative heights of boxes and move components around, as long as the connectivity between the different boxes is maintained, without changing the value of the diagram. For example, the following diagrams represent equal linear maps:




(12)

## 3.3 Finite sets

Given a finite set $S$, we can form the free complex vector space $\mathbb{C}[S]$, with a canonical basis in bijection with the elements of $S$. We equip this with an inner product such that the basis elements are orthonormal, giving rise to a Hilbert space. To reduce the weight of our notation, we allow the symbol $S$ to also stand for this Hilbert space, and write $|s\rangle$ to represent the basis element corresponding to the element $s$ of the original set.

An element of the Hilbert space is a formal linear combination of our basis elements, with complex coefficients. This representation allows us to define the linear maps $S \otimes S \xrightarrow{m} S$ and $\mathbb{C} \xrightarrow{u} S$, which form a commutative algebra:

$$m\left(\left(\sum_i a_i|i\rangle\right) \otimes \left(\sum_j b_j|j\rangle\right)\right) := \sum_k a_k b_k |k\rangle \tag{13}$$

$$u(1) := \sum_i |i\rangle \tag{14}$$

We represent these graphically in the following way.


(15)

Since these are linear maps between Hilbert spaces we can also construct their adjoints, which we denote as follows:

$$S \xrightarrow{m^\dagger} S \otimes S \qquad\qquad\qquad S \xrightarrow{u^\dagger} \mathbb{C} \tag{16}$$

These maps provide a canonical way to 'copy' and 'erase' elements of $S$, in a way which is governed by the canonical basis.

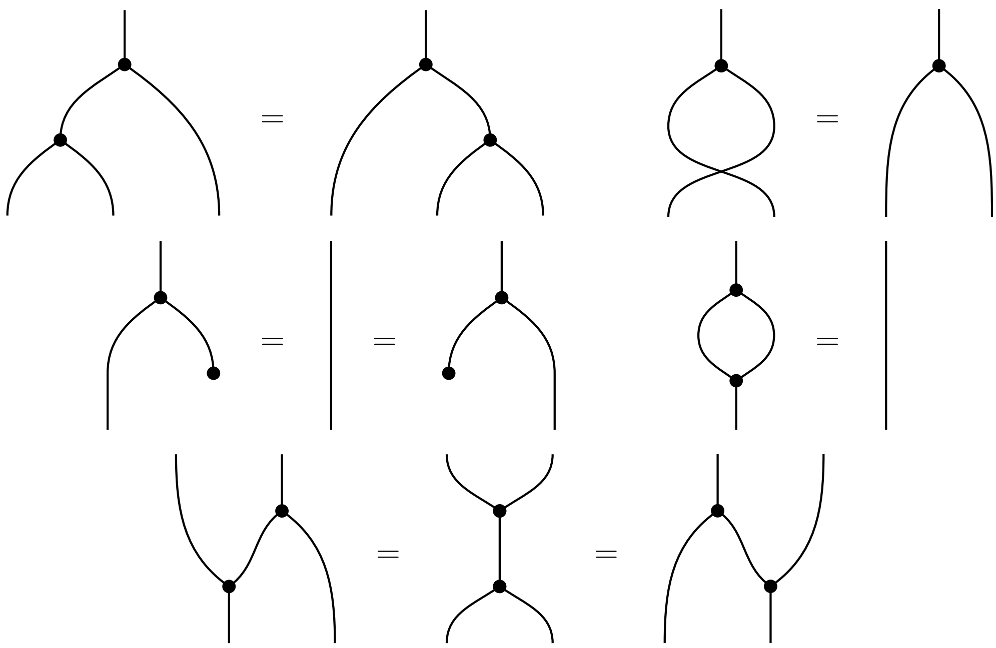
The relationships between composites of these are governed by a strong theorem [11, 16, 21].

**Theorem 3.1.** *Given a commutative algebra on a finite-dimensional Hilbert space $H$, the following are equivalent:*

1. *Any two composites of the multiplication, the unit and their adjoints, having the same inputs and outputs, are equal iff they have the same connectivity.*

2. *The algebra arises in the manner of equations* (13) *and* (14) *from an orthonormal basis of $H$.*

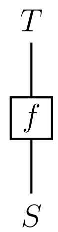
In particular, the following equalities are implied by these equivalent properties. Together these form the definition of a *classical structure*, also known as a *special †-Frobenius algebra*:



Conversely, these classical structure axioms imply property 1 of Theorem 3.1, a result known as the Spider Theorem [8].

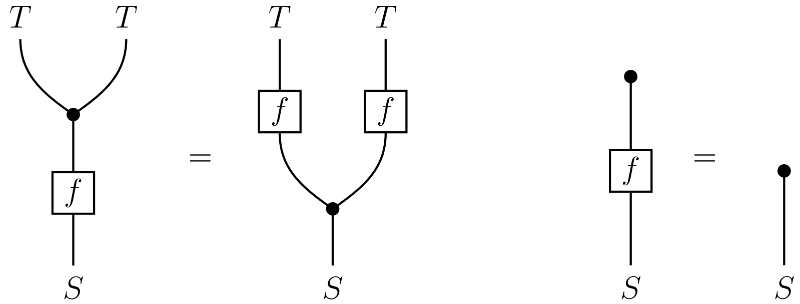
## 3.4 Functions between sets

A function $S \xrightarrow{f} T$ between finite sets extends to a linear map in a natural way, by defining $f|s\rangle := |f(s)\rangle$. We denote this graphically in the following simple way:




(17)

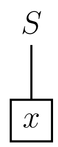
Linear maps arising in this way can be characterized in an elegant way using the graphical notation, as morphisms satisfying the following two conditions:




(18)

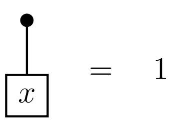
These are the *comonoid homomorphism* conditions. The first says that if you apply $f$ and then copy the result in the canonical basis of $T$, this is the same as copying the initial state in the canonical basis of $S$ and then applying $f$ to each branch. The second equation says that if you apply $f$ and then uniformly delete the result according to the canonical basis of $T$, the result is the same as simply deleting in the canonical basis of $S$.

A chosen element $x \in S$ corresponds to a function $1 \xrightarrow{x} S$, which gives rise to a linear map with the following graphical representation:



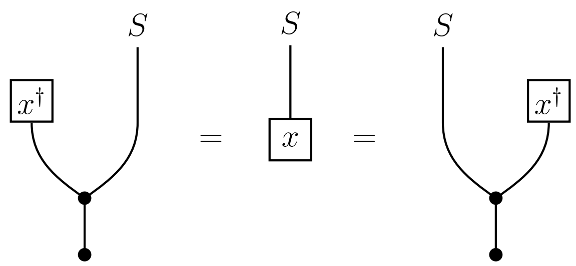

(19)

The deletion operation $u^\dagger$ introduced in (16) acts in the same way on all elements, reducing them to the unit scalar:




(20)

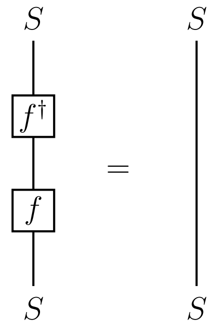
The linear map (19) is related to its adjoint in the following way:




(21)

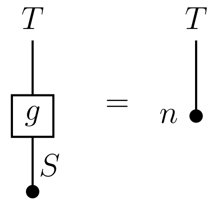
These equations say that the adjoint of (19) is its *dual*.

We can also use the topological calculus to express some simple features of particular linear maps. If a linear map $S \xrightarrow{f} T$ arises from a function between underlying sets in the manner described above, then this function is *injective* iff $f$ is an isometry, expressed by the following equation:




(22)

Surjectivity cannot be captured in quite such a straightforward way. However, suppose a linear map $S \xrightarrow{g} T$ arises from a function of underlying sets, and is *evenly surjective*, meaning the preimage of every basis element of $T$ has the same cardinality $n$. Then the following equation holds:



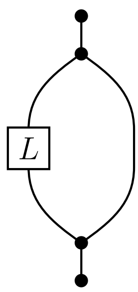

(23)

A lot more can be said on this topic, but these results are all we will need.

## 3.5 Traces

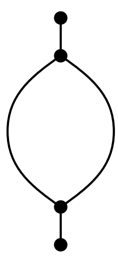
The topological algebra associated with the free Hilbert space $S$ on a finite set also allows us to describe taking traces of arbitrary linear maps $S \xrightarrow{L} S$. We define the trace graphically in the following way:

$\mathrm{Tr}(L) \quad =$




(24)

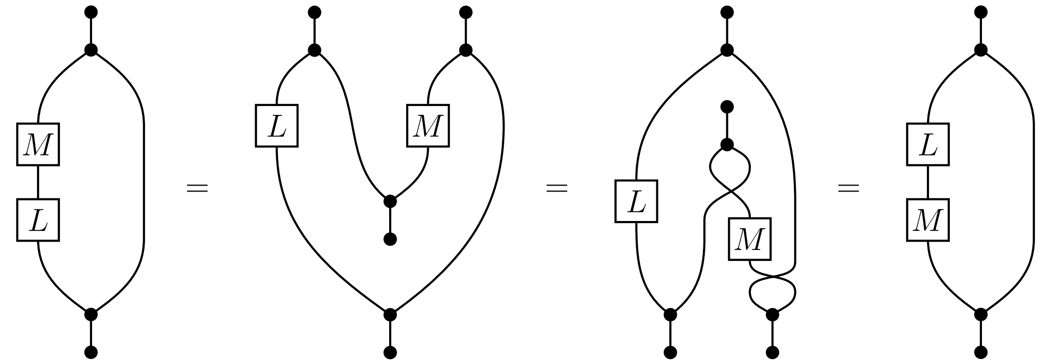
The trace of the identity gives the size of the set $S$:



$= \quad |S|$

(25)

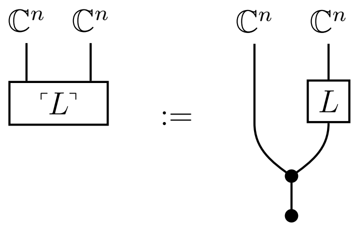
The formalism also allows a purely topological proof of the cyclic property:




(26)

## 3.6 Matrix algebras

The space of operators on a Hilbert space $\mathbb{C}^n$ is canonically isomorphic to $\mathbb{C}^n \otimes \mathbb{C}^n$. Given $\mathbb{C}^n \xrightarrow{L} \mathbb{C}^n$, we define its *name* $\ulcorner L \urcorner \in \mathbb{C}^n \otimes \mathbb{C}^n$ in the following way:

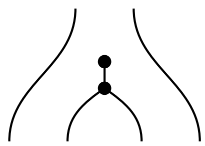



(27)

The correspondence between operators and their names is known in quantum information as the Choi-Jamiolkowski isomorphism. There is an algebra operation

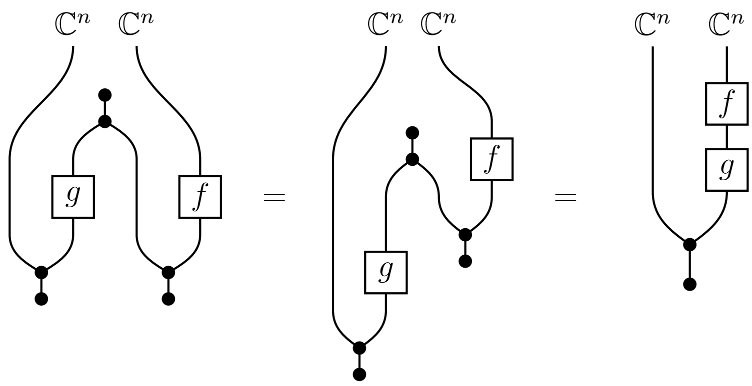
$$\mathrm{comp} : (\mathbb{C}^n \otimes \mathbb{C}^n) \otimes (\mathbb{C}^n \otimes \mathbb{C}^n) \to \mathbb{C}^n \otimes \mathbb{C}^n \tag{28}$$

on $\mathbb{C}^n \otimes \mathbb{C}^n$, which is the algebra $\mathrm{Mat}(n)$ of $n$-by-$n$ matrices. It is given by the following diagram:



(29)

This has the property that $\mathrm{comp}(\ulcorner g \urcorner, \ulcorner f \urcorner) = \ulcorner g \circ f \urcorner$, as the following graphical argument shows:




(30)

For convenience, we will use the following graphical simplifications:


(31)

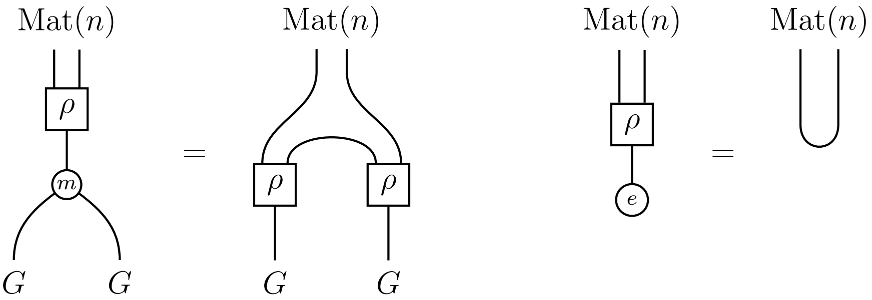
We will write $\mathrm{Mat}(n)$ and $\mathbb{C}^n \otimes \mathbb{C}^n$ interchangeably to refer to the matrix algebra we have described here.

## 3.7 Group representations

A group $G$ has a multiplication function $G \times G \xrightarrow{m} G$ and unit element $e \in G$, which we think of as a function $1 \xrightarrow{e} G$ from the 1-point set. Linearizing these, we denote them graphically in the following way:


(32)

In the case that $G$ is finite, its representations can be characterized as the maps $G \xrightarrow{\rho} \mathrm{Mat}(n)$ with the following topological properties:



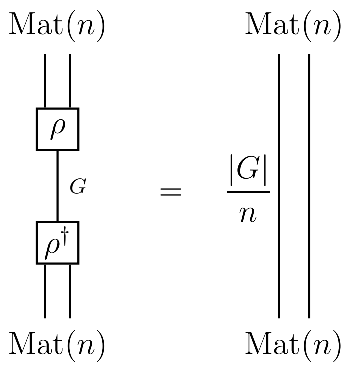

(33)

This says that $\rho$ is a homomorphism from the group algebra $G$ to the matrix algebra $\mathrm{Mat}(n)$, and is equivalent to the ordinary algebraic requirement for a representation that $\rho(gg') = \rho(g)\rho(g')$ for group elements $g, g' \in G$. We define $\mathrm{d}(\rho) := n$, the dimension of the vector space on which the representation acts.

## 3.8 Representations as projective measurements

For a finite group $G$, an irreducible representation $G \xrightarrow{\rho} \mathrm{Mat}(n)$ is proportional to a partial isometry, with scale factor $\sqrt{n/|G|}$.

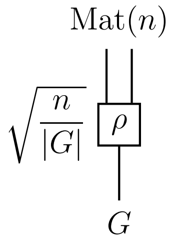
**Theorem 3.2.** *For a finite group $G$ and an irreducible representation $G \xrightarrow{\rho} \mathrm{Mat}(n)$, the following holds:*




(34)

*Proof.* A simple graphical transcription of Theorem A.3. ☐

The group algebra of a finite group is isomorphic to $\bigoplus_\rho \mathrm{Mat}(\mathrm{d}(\rho))$, where the sum is taken over equivalence classes of irreducible representations. As a result, the family of maps

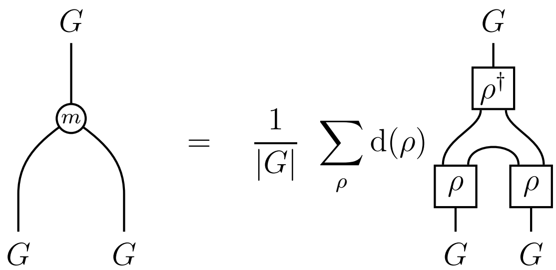



(35)

define a projective measurement on the group algebra. This will be degenerate in general, since for a nonabelian group not all irreducible representations are 1-dimensional.

## 3.9 Decomposing group algebras

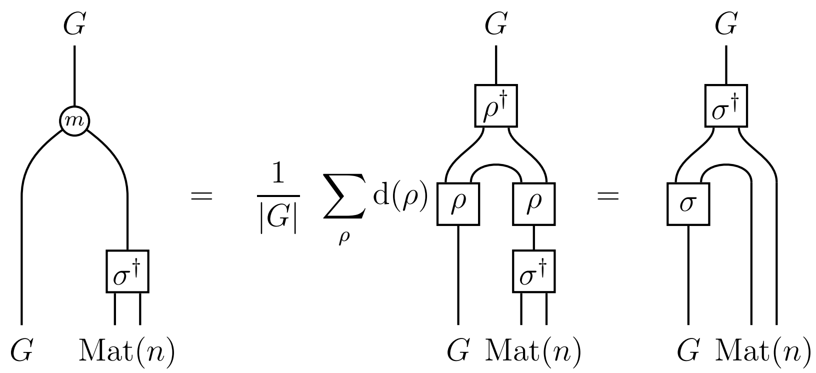
Group algebras are semisimple, which in the finite-dimensional case means that they are products of matrix algebras. By standard results from group representation theory, these matrix algebras are the matrix algebras on the irreducible representation spaces, where each equivalence class of irreducible representation is represented once. The multiplication operation for the group algebra can be decomposed in the following way, where the sum is over each equivalence class of irreducible representations, and where $|G|$ is the order of the group:




(36)

The general form of the right-hand side here can be deduced from the first property of (33), which says that each $\rho$ is an algebra homomorphism. The coefficients can then be obtained by applying Theorem 3.2.

We can use equation (36) to show that the multiplication vertex also copies irreducible representations when attached to either of the lower legs. For example, we obtain the following identity when composing $\sigma^\dagger$ onto the lower-right leg:




(37)

A similar expression holds for $\sigma^\dagger$ attached to the lower-left leg. Intuitively, the map $\sigma^\dagger$ is 'pulled through' the vertex $m$ when acting on one of the lower legs, extending the observation in (33) that representations are copied when composed at the target of the multiplication.

## 3.10 Normal subgroups

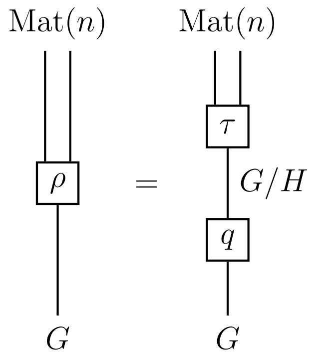
For a normal subgroup $H$ of a finite group $G$, we can construct a canonical projection

$$G \xrightarrow{q} G/H \tag{38}$$

from $G$ to the quotient group $G/H$. For an irreducible representation $G \xrightarrow{\rho} \mathrm{Mat}(n)$, exactly one of the following two topological facts is true.

**Theorem 3.3.** *For a projection $G \xrightarrow{q} G/H$ onto the quotient group of a normal subgroup $H \subseteq G$, then for an irreducible representation $G \xrightarrow{\rho} \mathrm{Mat}(n)$, exactly one of the following is true:*

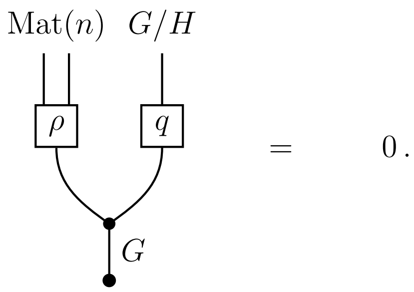
1. *The representation $\rho$ factors as*




(39)

   *for some irreducible representation $G/H \xrightarrow{\tau} \mathrm{Mat}(n)$.*

2. *The representation $\rho$ does not factor via $G \xrightarrow{q} \mathrm{Mat}(n)$ and*




(40)

*Proof.* Immediate from Theorems A.1 and A.2. □

# 4 Topological Deutsch-Jozsa

## 4.1 Introduction

We now present a new topological perspective on the Deutsch-Jozsa algorithm, making use of the topological formalism for algebra introduced in Section 3. This formalism will

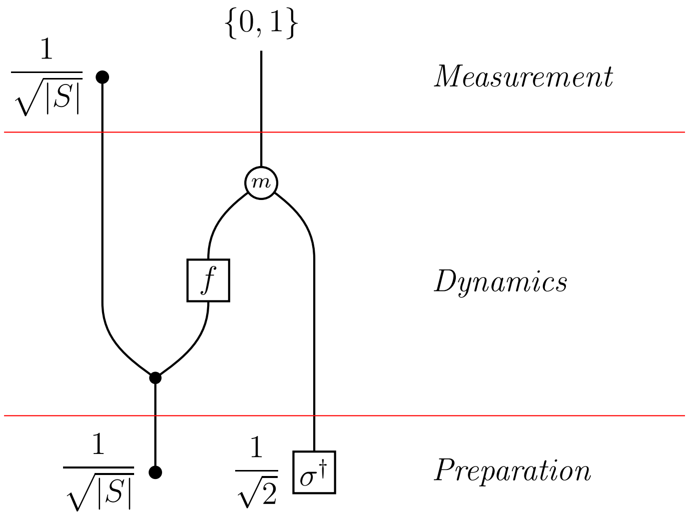
make clear many the mysterious features of the traditional presentation of the algorithm, as highlighted in the account in Section 2, by showing how the functionality of the algorithm is enabled by its topological structure.

The traditional presentation focused on properties of a function $\{0,1\}^N \xrightarrow{f} \{0,1\}$ between abelian groups. However, we argued that at no point in the protocol was the group structure on $\{0,1\}^N$ used in an essential way. For this reason, in our new perspective, we redefine our function to be of type

$$S \xrightarrow{f} \{0,1\} \tag{41}$$

where $S$ is a finite set.

The overall structure of the algorithm is given by the topological diagram below, in which time flows from bottom to top. The preparation, unitary dynamics and measurement phases are clearly indicated.




(42)

Over the course of this section we explain why this diagram represents the conventional Deutsch-Jozsa algorithm, and show how its form gives rise to a topological proof of correctness.

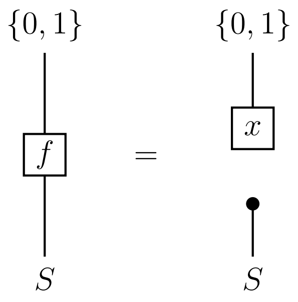
We end by showing how we can replace the group $\{0,1\}$ by an arbitrary finite group, and obtain a natural generalization of the Deutsch-Jozsa procedure. The algorithm we describe is close to that of Batty, Braunstein, Duncan and Høyer [14, 18], but strictly more general. As with the ordinary Deutsch-Jozsa algorithm, our primary contribution here is to demonstrate that the topological approach improves the proof of correctness significantly, making it shorter and easier to follow. We also have a substantial conceptual simplification: while the generalized Deutsch-Jozsa algorithm cited above could not have been developed without significant ingenuity and mathematical knowledge beyond that required to understand the original algorithm, in contrast, having understood our simple topological description of the Deutsch-Jozsa algorithm, the generalization is obvious, with the proof of correctness being almost immediate.

## 4.2 Constant and balanced functions

For the function $S \xrightarrow{f} \{0,1\}$ to be *constant* means that, as a function, it must factor via the 1-element set:

$$\begin{tikzcd} S \arrow[r] \arrow[rr, bend left, "f"] & 1 \arrow[r, "x"'] & \{0,1\} \end{tikzcd} \tag{43}$$

The function $S \to 1$ is the unique function to the 1-element set, and the function $1 \xrightarrow{x} \{0,1\}$ selects the element of $\{0,1\}$ which is the image of the function $f$. Linearizing these functions to produce linear maps between vector spaces, expression (43) has the following graphical representation:



(44)

The function $f$ is constant iff there exists some function $x$ satisfying this topological condition. Here we freely write $S$ and $\{0,1\}$ to represent the free complex vector spaces on these sets, and $f$ and $x$ for the linearizations of these functions, a notation which we will continue to use. Note that time flows from bottom to top here and in subsequent diagrams, in the style of the topological formalism introduced in Section 3, unlike the notation for the traditional circuit diagram (73) in which time flows from left to right.

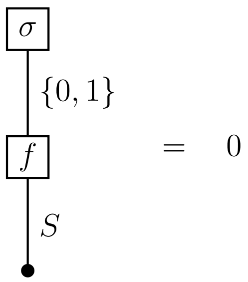
We now consider the case that $f$ is balanced. We can express this condition with the following equation:

$$\begin{pmatrix} 1 & -1 \end{pmatrix} \circ \sum_{s \in S} |f(s)\rangle = 0 \tag{45}$$

Composing with the matrix $\begin{pmatrix} 1 & -1 \end{pmatrix} : \{0,1\} \to \mathbb{C}$ contributes 1 to the sum for each element $s \in S$ with $f(s) = |0\rangle$, and $-1$ for each element with $f(s) = |1\rangle$. We can reexpress this equation as follows:

$$\begin{pmatrix} 1 & -1 \end{pmatrix} \circ f \circ \sum_{s \in S} |s\rangle = 0 \tag{46}$$

We can express this graphically using the formalism of Section 3, where we write $\sigma$ for the linear map $\{0,1\} \xrightarrow{(1\ -1)} \mathbb{C}$:

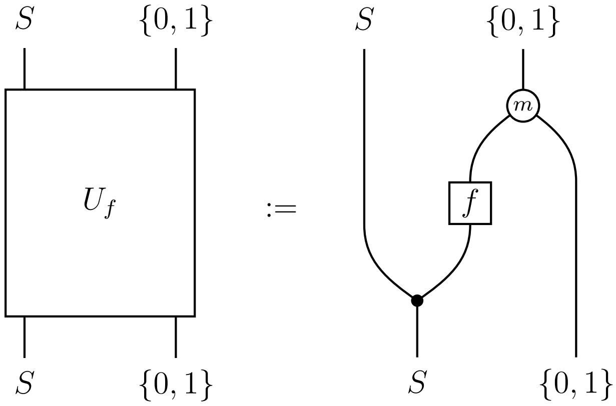


(47)

Equations (44) and (47) completely capture the constant and balanced properties using our topological algebra.

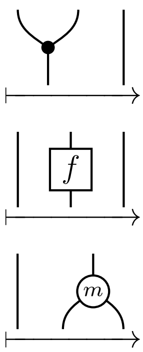
## 4.3 Building the unitary

At the heart of the Deutsch-Jozsa algorithm is the unitary operator $U_f$, with action defined by expression (3). We can define this topologically as follows:




(48)

To show this acts in the correct way, we evaluate its effect on a general input element, for some choice of $s \in S$ and $b \in \{0, 1\}$:

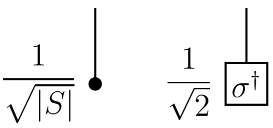



$$\begin{aligned} |s\rangle \otimes |b\rangle &\longmapsto |s\rangle \otimes |s\rangle \otimes |b\rangle \\ &\longmapsto |s\rangle \otimes |f(s)\rangle \otimes |b\rangle \\ &\longmapsto |s\rangle \otimes |f(s) \oplus b\rangle \end{aligned} \tag{49}$$

This matches our earlier definition.

## 4.4 Performing the algorithm

To obtain a topological expression for the result of the algorithm, we precompose our expression (48) with the choice of input state. The input states have the following graphical form:

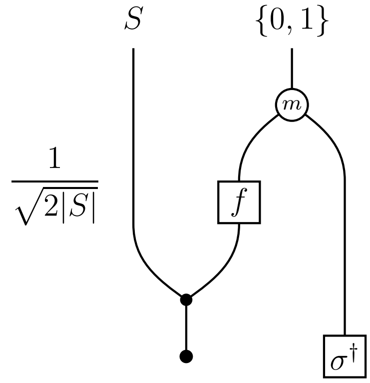



(50)

This expression includes the action of the Fourier transform operations on the input states of the traditional Deutsch-Jozsa circuit (73), which as we remarked in Section 2.2 have the effect of preparing the equal superposition state and the adjoint of the irreducible representation $\sigma$, up to a normalizing factor.

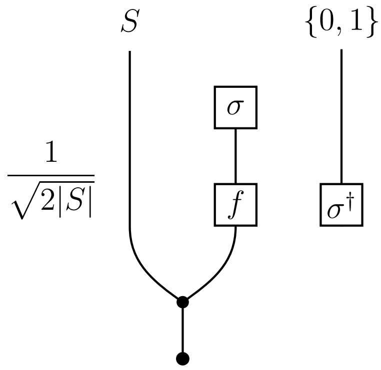
By composing expressions (50) and (48) we obtain the following topological expression for the quantum state after the protocol has been implemented, but before any

measurement is performed:



$$(51)$$

We omit the inverse Fourier transform present in the traditional circuit diagram (73) as we view it as forming part of the measurement. Due to property (37) of the multiplication vertex, we can rewrite this to obtain the following equivalent expression:

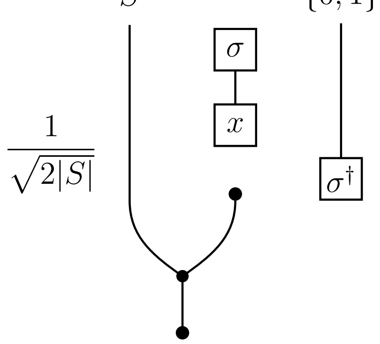


$$(52)$$

We see that the quantum state becomes a product state at this stage. We now examine the effect of a measurement on this state in the case that the function $f$ is constant or balanced.

## 4.5 Result when $f$ is constant

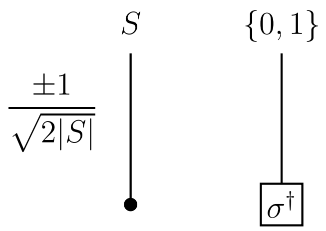
When $f$ is constant, we apply the topological equation (44) to rewrite expression (52) for the quantum state after the unitary evolution stage of the algorithm has been completed, obtaining the following diagram:



$$(53)$$

The composite $\sigma \circ x$ represents the value of the irreducible representation $\sigma$ on the element $x \in \{0,1\}$ which is the image of the function $f$. Since $\sigma = \begin{pmatrix} 1 & -1 \end{pmatrix}$, this composite

equals $\pm 1$. Using this fact, along with the properties of the topological algebra on a finite set, we simplify diagram (54) to obtain the following expression:

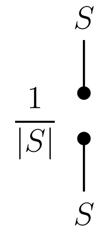



(54)

This is a product state, with the left-hand family of qubits in the superposition state (5). As a result, the projective measurement performed onto the superposition state is guaranteed to be successful. This demonstrates that, in the case that $f$ is constant, we will measure the system $S$ to be in the superposition state (5) with certainty.

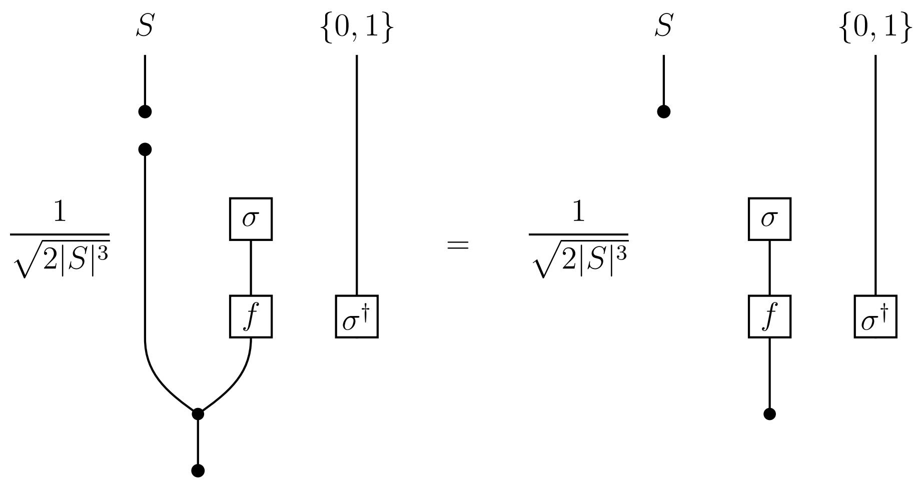
## 4.6 Result when $f$ is balanced

We now consider the result of a measurement of the left-hand system in the superposition state (5) in the case that $f$ is balanced. The following diagram represents a projector onto the 1-dimensional subspace of $S$ corresponding to the uniform superposition state:




(55)

Applying this to expression (52) representing the quantum state after the main body of the algorithm has been performed, and then simplifying the result, we obtain the following diagram:




(56)

By equation (47) defining the case when $f$ is balanced, we see that this composite is equal to 0. We conclude that, in this case, there is no possibility of measuring the system $S$ to be in the uniform superposition state (5). This completes the topological demonstration of correctness of the Deutsch-Jozsa algorithm.

## 4.7 Generalization to arbitrary finite groups

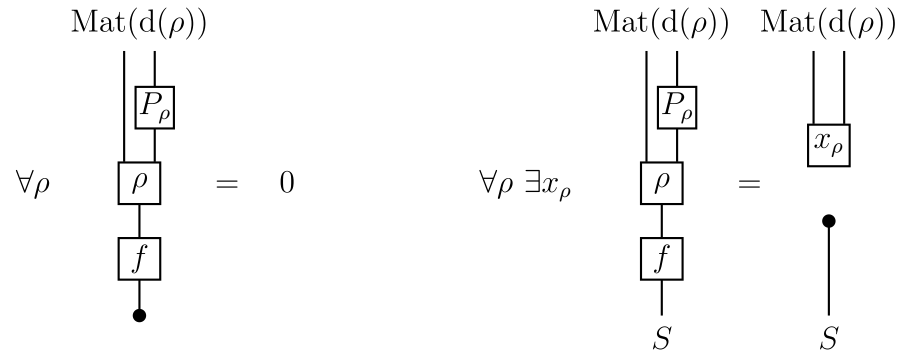
Our topological approach allows the Deutsch-Jozsa to be easily generalized from the group $\{0,1\}$ to arbitrary groups $G$. Our function then takes the form

$$S \xrightarrow{f} G\,. \tag{57}$$

In the traditional Deutsch-Jozsa algorithm described earlier in this section, the alternating representation $\{0,1\} \xrightarrow{\sigma} \mathbb{C}$ plays a central role. In this generalization we replace it with an arbitrary irreducible representation $G \xrightarrow{\rho} \mathrm{Mat}(n)$, where $n$ is the dimension of the representation. We continue our tradition of viewing the symbol $G$ as representing both a finite group and the free vector space $\mathbb{C}[G]$ depending on context. The concepts of constant and balanced functions will also be generalized, in a way which we will see below.

The generalization of the Deutsch-Jozsa algorithm presented here is closely related to that of Batty, Braunstein, Duncan and Høyer [14, 18]. We believe our formulation is strictly more general. In addition, thanks to the topological calculus, the proof of correctness is only a couple of pages, rather than the many pages required in these references. The topological formalism also makes it clear exactly *why* the generalized algorithm is successful.

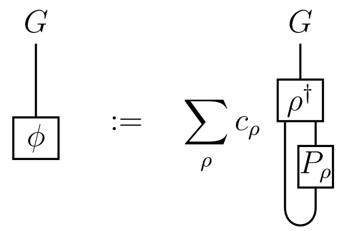
We begin by defining generalizations of the constant and balanced properties. For each isomorphism class of irreducible representation $\rho$, in which the group acts on the Hilbert space $V_\rho$, we pick an orthogonal projector $V_\rho \xrightarrow{P_\rho} V_\rho$ onto some subspace, such that at least one of these projectors is nonzero. With respect to such a family $P_\rho$ of projectors, we make the following definitions of the properties $P_\rho$-*balanced* and $P_\rho$-*constant*:



(58)

$P_\rho$-balanced $\qquad\qquad$ $P_\rho$-constant

We then define an element $\phi$ of the group algebra of $G$ in the following way:

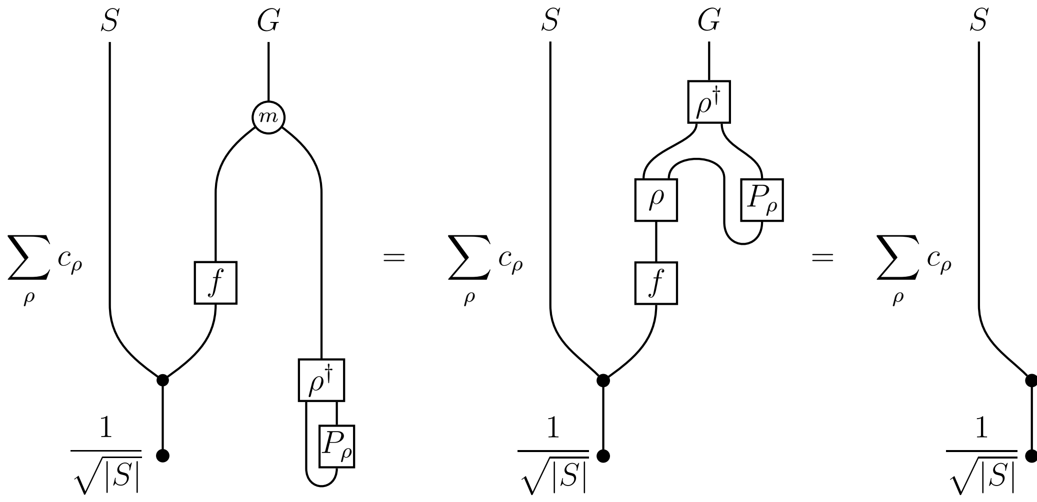


(59)

The summation is over the equivalence classes of irreducible representations $\rho$ of $G$. The coefficients $c_\phi$ are arbitrary but nonzero, and can always be picked to ensure that $\phi$ has norm 1. It is here that our procedure is more general than that of Batty, Duncan and

Braunstein [18], who require a single $P_\rho$ to have rank 1, and all others to have rank 0. Also, they require the nonzero projector to have support given by a particular basis element of the representation space.

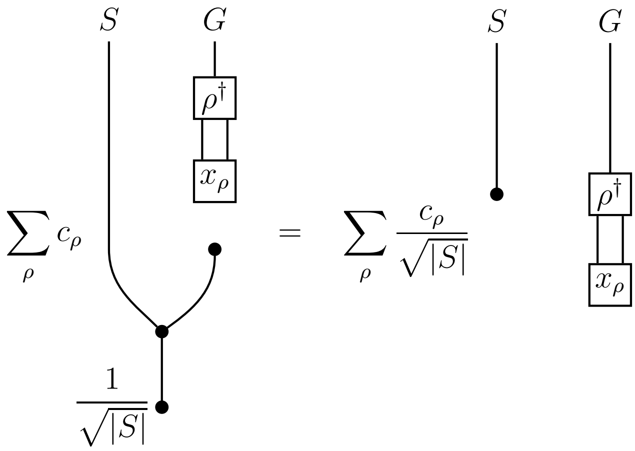
Our generalized Deutsch-Jozsa algorithm proceeds as in the standard case described earlier in this section, except we use this state $\phi$ as the initial state for the system $G$. After the unitary dynamics step, the state of the system has the following topological form:



(60)

We are now ready to consider the measurement stage of the protocol, which is a projective measurement onto the even superposition state of $S$.

Suppose that $f$ is $P_\rho$-constant. Then using equation (58) we obtain the following expression for the overall state:

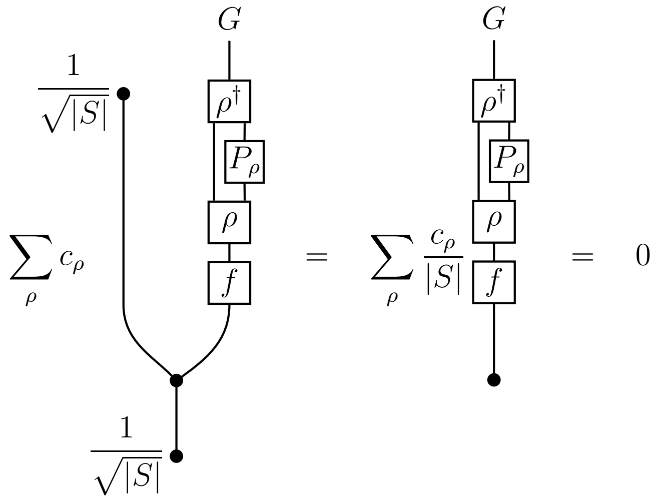


(61)

This is a product state, with the system $S$ in the even superposition state. A projective measurement onto this state is therefore guaranteed to be successful.

Finally, suppose that $f$ is $P_\rho$-balanced. To determine the effect of a projective measurement onto the even superposition state, we compose (82) with a partial isometry

onto that subspace of the system $S$:




(62)

Using the definition (58) of a $P_\rho$-balanced function, this composite is zero, so we have shown that in the $P_\rho$-balanced case there is no possibility of measuring the system $S$ in the even superposition state.

# 5 The hidden subgroup algorithm

## 5.1 Introduction

The hidden subgroup family of algorithms is rich, containing Deutsch's original algorithm, as well as Simon's algorithm and Shor's algorithm. We use our topological notation to prove correctness of the algorithm, and clarify its structure.

We are given a function $G \xrightarrow{f} X$, promised to be constant on the cosets of some normal subgroup $H \subseteq G$, and distinct otherwise. This says exactly that the function $f$ factorizes as

$$\begin{tikzcd} G \arrow[r, two heads, "q"'] \arrow[rr, bend left, "f"] & G/H \arrow[r, tail, "s"'] & S \end{tikzcd}, \tag{63}$$

where $q$ is a surjective projection onto the quotient group $G/H$, and $s$ is an embedding into some set. The algorithm determines the subgroup $H$ in $O(\log |G|)$ trials.

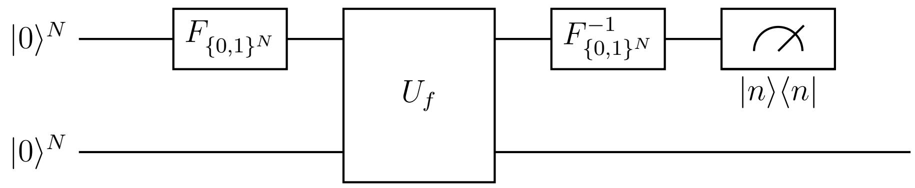
Traditionally applied only in the case where $G$ is abelian, it was extended to the case of normal subgroups of arbitrary finite groups by Hallgren, Russell and Ta-shma [13]. It is this generalized version that we treat here. Our approach gives a clean separation between the group-theoretical and quantum aspects of the protocol, and yields a proof of correctness which is simpler, shorter, and easier to follow.

We begin with a brief account of the traditional presentation of the algorithm, again highlighting features which seem unclear from this perspective.

## 5.2 Traditional version

Here we give the conventional presentation of the algorithm as usually encountered, which determines a hidden subgroup of an abelian group [19]. For concreteness we choose

the special case commonly known as Simon's algorithm [23], specified by $H = \{0,1\}$, $G = \{0,1\}^N$ and $S = \{0,1\}^N$. The following circuit diagram gives the procedure:




(64)

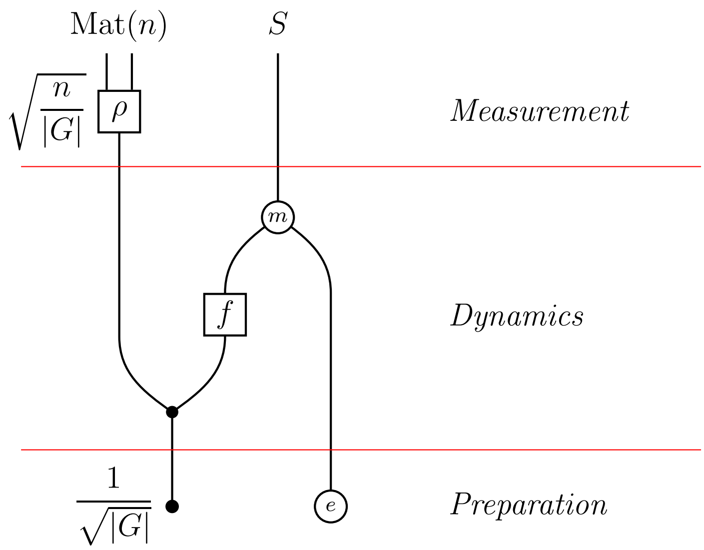
We have two families of qubits, both of which are prepared in the state $|0\rangle^N$. We then perform a Fourier transform on the first family, followed by the unitary operator $U_f$, and an inverse Fourier transform on the first family. The unitary $U_f$ at the centre is identical to that used by the Deutsch-Jozsa algorithm, as described in Section 2.1. Finally, we perform a projective measurement of the first system in the computational basis, with some nondeterministic outcome $|n\rangle$. An analysis of this procedure shows that the only values $n \in \{0,1\}^N$ that can be measured are those for which $h \cdot n = 0$, where $h \in \{0,1\}^N$ is the nontrivial element of the hidden subgroup $\{0,1\} \subset \{0,1\}^N$, and the binary operation is inner product modulo 2.

Via the inverse Fourier transform $F^{-1}_{\{0,1\}^n}$ the element $n$ in fact corresponds to some irreducible representation $\{0,1\}^N \xrightarrow{\omega_n} \mathbb{C}$, and in these terms the inner product condition becomes the requirement that $\omega_n(h) = 1$. In words: we can only measure those $n$ such that the corresponding representation $\omega_n$ restricts to the trivial representation on the hidden subgroup. It is this property that we will demonstrate directly using the topological formalism.

As with the Deutsch-Jozsa algorithm, there are features which are not clear from this presentation. The structure of the algorithm is opaque: it is not clear how or why the components of the algorithm work together to give the correct outcome. Presentations of the algorithm are inconsistent, with a measurement on the lower system sometimes also specified. Finally, is it not clear how the algorithm can be generalized. Our topological version of the hidden subgroup algorithm illuminates these issues, for the general case of a normal subgroup of an arbitrary finite group.

## 5.3 Topological version

The following diagram summarizes our topological account of the algorithm.

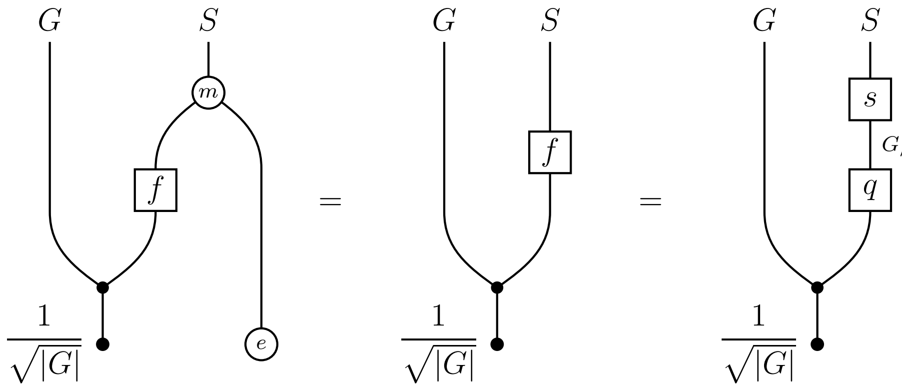



(65)

We begin by preparing two systems: one with state space give by a group algebra $G$ in the uniform superposition state; and another with state space given by a set $S$ in some basis state $|e\rangle$. We then perform the unitary dynamics described by the second section, which as described in Section 4.3 recreates the action of the unitary operator $U_f$ in the conventional presentation. For this purpose we require a group structure on $S$: we choose any structure such that $e$ is the identity element.

The procedure finishes with a measurement on the first system in the partition defined by the irreducible representations, as described in Section 3.8. Using a topological encoding of a result from group theory, we demonstrate that the only representations that can be successfully measured are those which arise as restrictions of representations of the quotient group $G/H$. Classical postprocessing then suffices to deduce the subgroup $H$ in $O(\log |G|)$ trials [13].

After the unitary dynamics step, the system is in the following state:




(66)

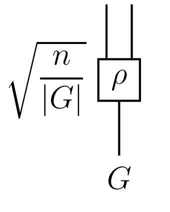
These are topological representations of the following algebraic expression:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \,. \tag{67}$$

On the right-hand side of (66) we have rewritten $f$ in terms of its promised factorization (63) via an unknown quotient group $G/H$.

## 5.4 Performing the measurement

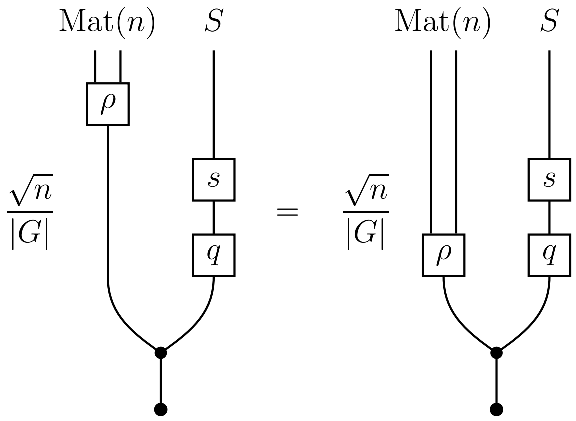
We now describe measurement of the first system $G$, using a projective measurement determined by the irreducible representations. To understand what results are possible, we compose the state (66) with the linear map




(68)

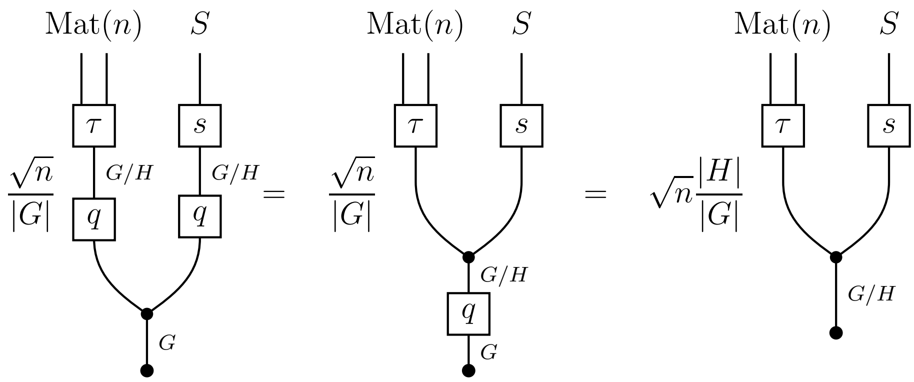
on the first factor, which as discussed in Section 3.8 is a partial isometry projecting onto the subspace of the group algebra corresponding to the irreducible representation $\rho$. This

gives the following result:



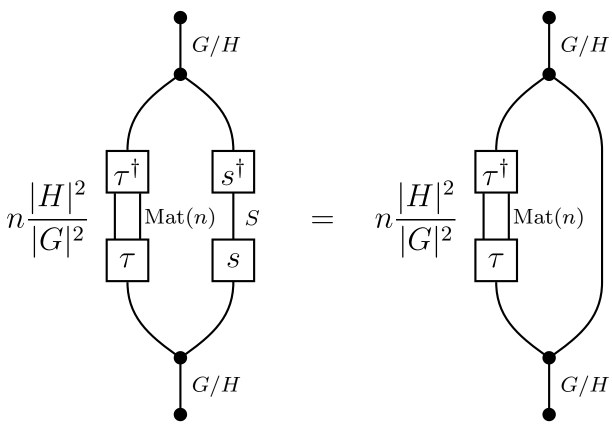

(69)

By Theorem 3.3, this is zero exactly when $\rho$ does not factor through the unknown quotient group $G/H$. So the only irreducible representations that can be measured in this way are those which factorize as $G \xrightarrow{q} G/H \xrightarrow{\tau} \mathrm{Mat}(n)$, for some irreducible representation $\tau$ of $G/H$. In this case, our projected state (69) can be rewritten as follows, making use of the topological properties of functions between basis elements and even surjections as presented in Section 3.4:

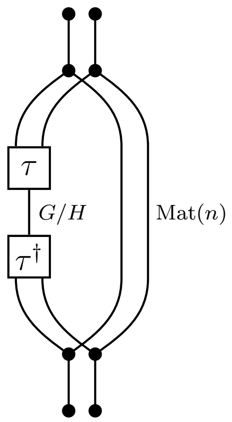



(70)

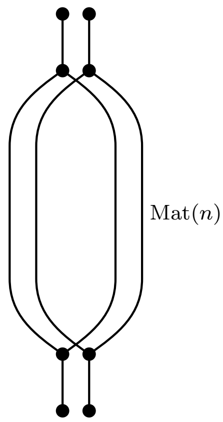
We calculate the norm of this state in the following way, employing the graphical characterization of injective functions given in Section 3.4, and both the cyclic property of the trace and the topological expression of the dimension of a vector space as developed in Section 3.5:



$= n\frac{|H|^2}{|G|^2}$




$= \frac{|H|}{|G|}$




$= \frac{|H|}{|G|}n^2 \qquad (71)$

So the measurement will return exactly those irreducible representations of $G$ that factor through the unknown quotient group $G/H$, with a probability proportional to the square of the dimension of the representation. Classical postprocessing can then determine the hidden subgroup in $O(\log|G|)$ trials [13].

# 6 Grover's algorithm

## 6.1 Introduction

In this section we give a topological analysis of a deterministic instance of Grover's algorithm, which is used to search a set $S$ for marked elements, defined in terms of an indicator function

$$S \xrightarrow{f} \{0, 1\}$$

onto the group of integers under addition modulo 2. Grover's algorithm is nondeterministic in general, which makes it difficult to treat in our formalism. We restrict attention to the deterministic case in which a single iteration of the algorithm guaranteed to return a marked element. This corresponds to the case that exactly $\frac{1}{4}$ of the elements are marked. Our topological analysis makes it clear why Grover's algorithm is always successful in this case.

We then explore a generalization of Grover's algorithm, made natural by our approach, in which our set $S$ is equipped with a function to an arbitrary finite group. We demonstrate that this generalized algorithm is guaranteed to return an *unbalanced* element of $S$ after a single iteration. Given an irreducible representation $\rho$ of $G$, we define the element $s \in S$ to be *balanced* if the following holds:

$$\rho(f(s)) = \frac{2}{|S|}\sum_{t\in S}\rho(f(t)) \qquad (72)$$

In words, an element $s \in S$ is balanced if $\rho(f(s))$ equals twice the average value, using the uniform measure on $S$. If an element is not balanced, then it is *unbalanced.*

To illustrate this, consider the case of $G = \mathbb{Z}_3$, and write [6] for the set $\{1, 2, 3, 4, 5, 6\}$. Consider the function $[6] \xrightarrow{f} \mathbb{Z}_3$ defined as follows:

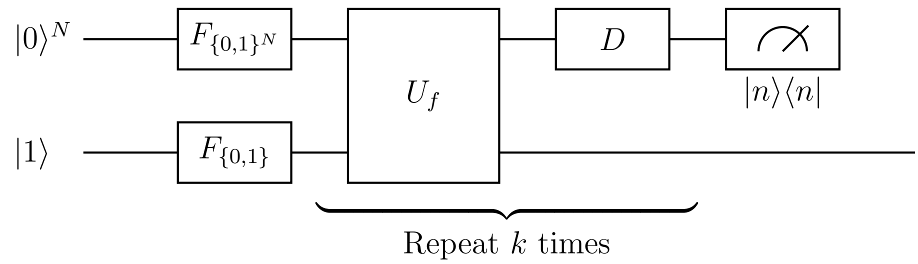
$$\begin{array}{lll} f(1) = 0 & f(5) = 1 & f(6) = 2 \\ f(2) = 0 & & \\ f(3) = 0 & & \\ f(4) = 0 & & \end{array}$$

We choose the representation $\mathbb{Z}_3 \xrightarrow{\rho} \mathbb{C}$ with $\rho(1) = e^{2\pi i/3}$. Under this representation, the average value of the quantity $\rho(f(n))$ over all $n \in [6]$ is $\frac{1}{2}$. As a result, the elements 0, 1, 2 and 3 are balanced, since for these values $\rho(f(n))$ is twice the average value. The elements 4 and 5 are unbalanced, so these are the only possible measurement outcomes.

This procedure is useful if we are given a function $S \xrightarrow{f'} \mathbb{Z}_3$ promised to be of the form $S \xrightarrow{\sim} S \xrightarrow{f} \mathbb{Z}_3 \xrightarrow{\sim} \mathbb{Z}_3$, where the first and last arrows are bijections. Our generalized Grover search algorithm will return an unbalanced element of $S$ in a single query for *all* these functions. This cannot be handled by the standard Grover algorithm. If we knew beforehand what values of $G$ are taken by the unbalanced elements of $S$ (in our example, 1 and 2), and if we knew the fraction of elements which are unbalanced (in this case $\frac{1}{3}$), then we could compose $f$ with a function to $\mathbb{Z}_2$ that takes $0 \mapsto 0$, $1 \mapsto 1$ and $2 \mapsto 1$, and apply an optimal variant of Grover's conventional search algorithm to find a rare element with certainty after a single iteration [5]. However, in general, this information will not be known.

## 6.2 Traditional presentation

Grover's algorithm is traditionally presented in terms of the following circuit diagram:




(73)

A family of $N$ qubits is prepared in the product state $|0\rangle^N$, to which a Fourier transform is applied, giving the uniform superposition state. A second qubit is prepared in the state $|1\rangle$, on which a Fourier transform acts to give the state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The unitary $U_f$ as defined by equation (3) is then applied, followed by a Grover diffusion operator $D$ on the first family of qubits, defined in the following way:

$$D|m\rangle = |m\rangle - \frac{1}{2^{N-1}} \sum_{0 \le n \le 2^N - 1} |n\rangle$$

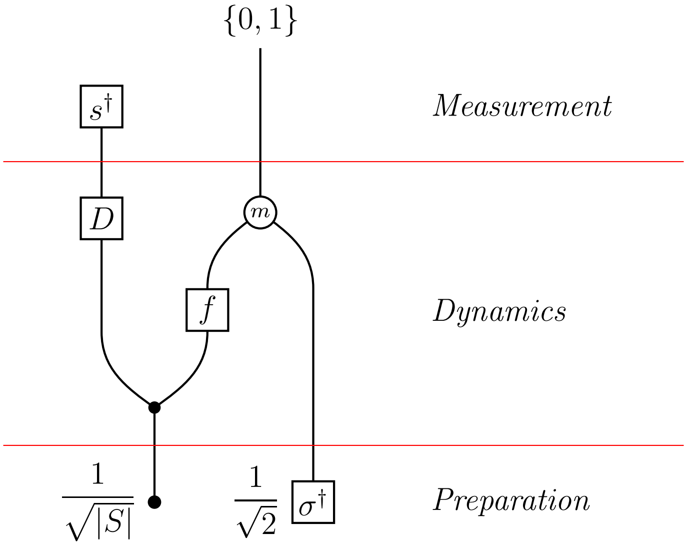
The composite $(D \otimes \mathrm{id}_{\mathbb{C}^2}) \circ U_f$ is referred to as a single Grover step, and in general is repeated some particular number of times depending on the properties of the function $f$. Finally, a measurement is performed on the first family of $n$ qubits in the computational basis.

As with the other algorithms we consider in this paper, this traditional presentation does not make clear why the algorithm should be successful. The particular choices of initial states, the form oracle $U_f$ and the diffusion operator $D$ together produce the desired effect, but no high-level structure is available that can account for the algorithm's success, and the only way that correctness can be demonstrated is to perform the required low-level linear algebraic calculations.

## 6.3 Topological presentation

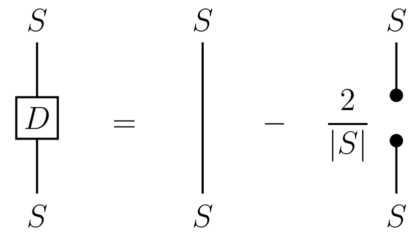
Our topological perspective demonstrates why Grover's algorithm is successful in the deterministic case, where exactly a quarter of the elements are marked, and the Grover

step is executed once. The overall topological structure of the algorithm is as follows:



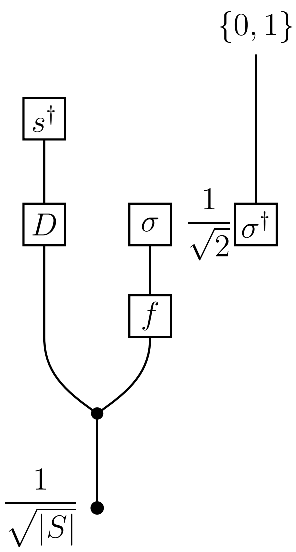

(74)

This represents the final state after a successful projective measurement of the first system in the basis state $|s\rangle$. Furthermore, we can decompose $D$ in the following way, as a linear combination of two other diagrams:



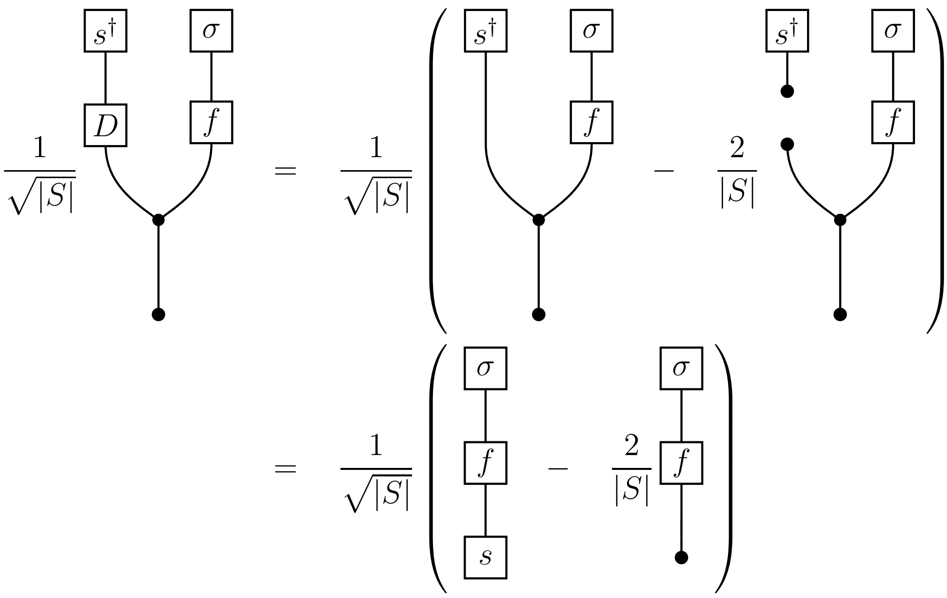

(75)

This allows us to perform a completely topological analysis of the algorithm. By equation (37), the linear map $\sigma^\dagger$ is duplicated by the group multiplication vertex $m$ in equation (79), allowing us to rewrite it in the following way:




(76)

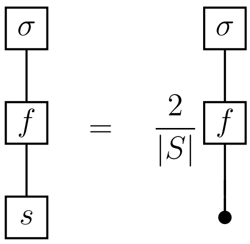
Since this is a product state, we can neglect the second system, rewriting the state of the first system using the topological decomposition (75) of the diffusion operator $D$:



(77)

In the final equality we use properties of the topological algebra of finite sets, as described in Sections 3.3 and 3.4.

This is zero for those $s \in S$ satisfying the following equation:



(78)

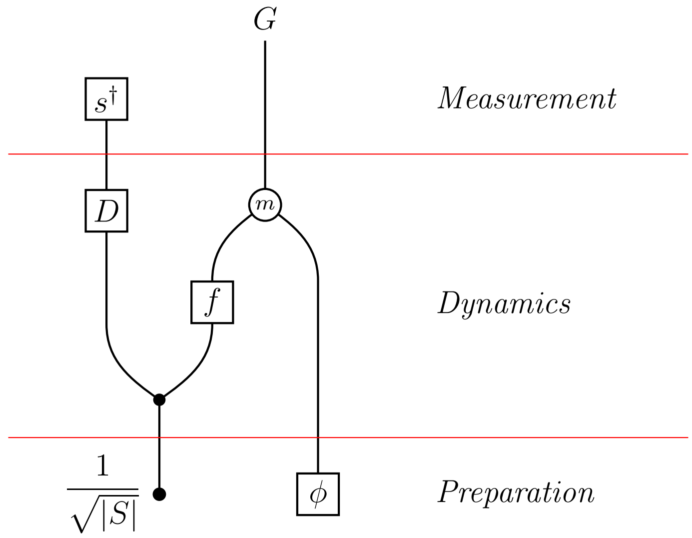
Such an $s$ cannot be the result of a measurement. The right-hand side of this expression represents twice the average value of the function $f$ under the representation $\sigma$. The left-hand side represents the value of the function $f$ at the element $s$, under the representation $\sigma$. If this left-hand side is equal to $+1$, it is straightforward to see that $f$ must take the value 1 on three-quarters of the elements of $S$. If the left-hand side is equal to $-1$, then $f$ must take the value 1 on one-quarter of the elements of $S$.

This recovers the standard result from Grover search: to find a marked element with certainty after a single step, exactly a quarter of elements must be marked. Note that standard Grover theory assumes that the marked elements take the value 1 under the function $f$, but this is not required: the unmarked elements could just as well take the value 1, and the marked elements the value 0. It is clear that these two cases give rise to essentially the same procedure, since the difference corresponds to an overall phase.

## 6.4 Generalization

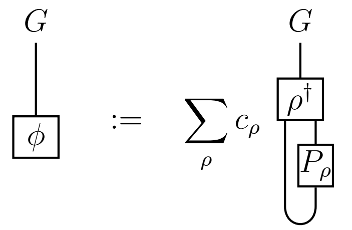
We generalize this by replacing the group $\{0, 1\}$ with an arbitrary finite group $G$. Loosely, the generalized algorithm guarantees to find an element $s \in S$ for which $\rho(f(s))$ does not take twice its average value, restricted to some chosen subspace of the representation

space. The following diagram gives a topological outline of the algorithm:



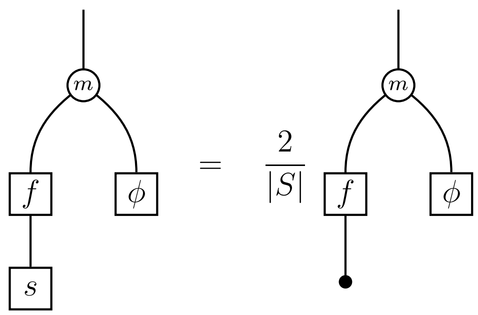

(79)

The system $G$ is initialized in a state $\phi$ which is chosen in the following way, just as with the generalized Deutsch-Jozsa algorithm presented in Section 4.7:




(80)

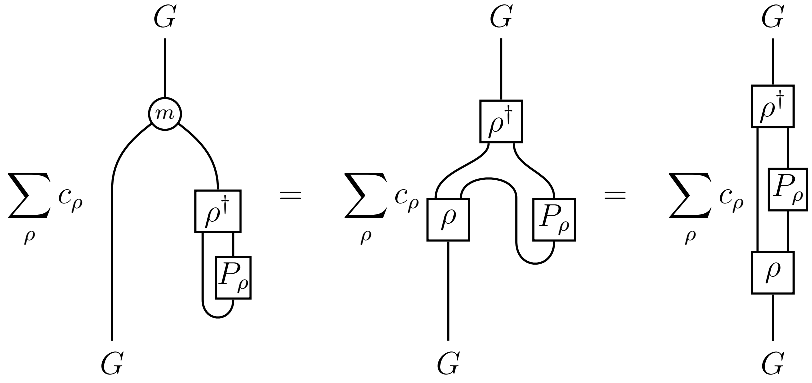
The algorithm proceeds by choosing some element $\phi \in G$ of the group algebra as an initial state. By following a similar argument to the previous section, we obtain the following expression for the basis elements $|s\rangle \in S$ which have zero amplitude to be measured:




(81)

From this equation, we see that the algorithm will never return those elements $s \in S$ such that, restricted the support of $m(-, \phi)$, the group element $f(s)$ takes twice its average value. We can apply definition (80) to see how $m(-, \phi)$ acts in terms of our chosen

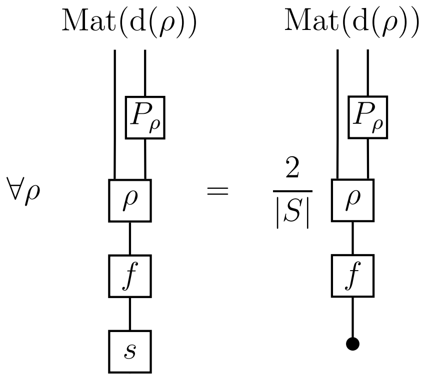
projectors $P_\rho$:




(82)

The support of this operator is the union of subspaces defined by our projectors $P_\rho$, across all the equivalence classes of irreducible representations.

Applying this to equation (81), we see that a basis element $|s\rangle \in S$ cannot be the result of the measurement if it satisfies the following condition, which generalizes condition (78) above for a balanced element of $S$:




(83)

This says that, under each representation $\rho$, restricted to the subspace $\mathrm{id}_{\mathrm{d}(\rho)} \otimes P_\rho$, the group element $f(s)$ takes twice its average value.

# A Results in group theory

## A.1 Introduction

In this appendix we collect proofs of some standard results in the theory of finite groups, which are of use as part of our main presentation.

## A.2 Normal subgroups

**Theorem A.1.** *For a normal subgroup $H$ of a finite group $G$, and an irreducible representation $G \xrightarrow{\rho} GL(n)$, exactly one of the following properties holds:*

1. *The representation factors via the quotient group $G/H$ and*

$$\sum_{h \in H} \rho(h) = |H| \, \mathrm{id}_n;$$

*2. The representation does not factor via the quotient group $G/H$ and*

$$\sum_{h\in H}\rho(h)=0.$$

*Proof.* Suppose that $\rho$ restricts to a trivial representation on $H$. Then $\rho(g)=\rho(g)\rho(h)=\rho(gh)$ for all $g\in G$ and $h\in H$, so $\rho$ is well-defined on cosets, and factors via the quotient group $G/H$. So property 1 holds, and property 2 is clearly false.

Otherwise, suppose that $\rho$ does not restrict to a trivial representation on $H$. So both parts of property 1 must be false. By Clifford's theorem [4] the restricted representation $\rho_H$ is of the form

$$\rho_H(h)=\bigoplus_i \sigma\big(g_i h g_i^{-1}\big) \tag{84}$$

where $\sigma$ is an irreducible representation of $H$, and where $g_i$ is some finitely-indexed family of elements of $G$, such that the summands are pairwise nonisomorphic representations. None of these summands can be the trivial representation, since then they would all be trivial, which would violate our hypothesis. Thus $\rho_H$ does not contain the trivial representation as a subrepresentation. Property 2 of the theorem follows, since $\sum_{h\in H}\rho(h)$ is proportional to a projector onto a trivial subrepresentation. $\square$

**Theorem A.2.** *For a projection $G\xrightarrow{q}G/H^l$ onto the left coset space of a subgroup $H\subseteq G$, then for a representation $G\xrightarrow{\rho}GL(n)$*

$$\sum_{h\in H}\rho(h)=0 \quad\Rightarrow\quad \sum_{g\in G}\rho(g)\otimes q(g)=0\,. \tag{85}$$

*Proof.* For a subgroup $H\subseteq G$, we can choose a representative $g_c\in G$ for each element of the coset space $c\in G/H^l$, such that every element $g\in G$ is uniquely of the form $hg_c$ for some $c\in G/H$ and $h\in H\subseteq G$, and such that $q(g_c)=c$. As a result, the sum of property 2 above can be rewritten as

$$\sum_{h\in H}\sum_{c\in G/H}\rho(hg_c)\otimes q(g_c)=\left(\left(\sum_{h\in H}\rho(h)\right)\otimes \mathrm{id}_{G/H}\right)\circ\left(\sum_{c\in G/H}\rho(g_c)\otimes c\right) \tag{86}$$

This makes the implication clear. $\square$

## A.3 Normalization of irreducible representations

**Theorem A.3.** *For a finite group $G$ and an irreducible representation $G\xrightarrow{\rho}\mathrm{Mat}(n)$,*

$$\rho\circ\rho^\dagger=\frac{|G|}{n}\,\mathrm{id}_{\mathrm{Mat}(n)}\,. \tag{87}$$

*Proof.* Since irreducible representations are surjective as functions on the group algebra, it suffices to show

$$\rho\circ\rho^\dagger\circ\rho=\frac{|G|}{n}\rho\,,$$

and since the group elements form a basis for the group algebra, it is enough to show that for all $g\in G$

$$\rho\circ\rho^\dagger\circ\rho(g)=\frac{|G|}{n}\rho(g)\,.$$

From the definition

$$\langle g|\rho^\dagger(M)\rangle_G = \langle \rho(g)|M\rangle_{\mathrm{Mat}(n)} = \mathrm{Tr}(\rho(g^{-1}) \circ M)$$

we see that

$$\rho^\dagger(M) = \sum_{h\in G} \mathrm{Tr}(\rho(h^{-1}) \circ M)\, |h\rangle\,,$$

which for $M = \rho(g)$ gives

$$\begin{aligned}
\rho \circ \rho^\dagger \circ \rho(g) &= \sum_{h\in G} \mathrm{Tr}(\rho(h^{-1}) \circ \rho(g))\rho(h) \\
&= \sum_{h\in G} \mathrm{Tr}(\rho((gh)^{-1}) \circ \rho(g))\rho(gh) \\
&= \rho(g) \sum_{h\in G} \mathrm{Tr}(\rho(h^{-1}))\rho(h)\,.
\end{aligned} \tag{88}$$

Consider the element $X := \sum_{h\in G} \mathrm{Tr}(\rho(h^{-1}))\rho(h)$ of $\mathrm{Mat}(n)$. It is an intertwiner for the irreducible representation $\rho$, since

$$\begin{aligned}
X \circ \rho(g) &= \sum_{h\in G} \mathrm{Tr}(\rho(h^{-1}))\rho(h) \circ \rho(g) \\
&= \sum_{h\in G} \mathrm{Tr}(\rho(h^{-1}))\rho(hg) \\
&= \sum_{h'\in G} \mathrm{Tr}(\rho(gh'^{-1}g^{-1}))\rho(gh'g^{-1}g) \qquad \text{(for } h \mapsto gh'g^{-1}\text{)} \\
&= \rho(g) \sum_{h'\in H} \mathrm{Tr}(\rho(h'^{-1}))\rho(h') \\
&= \rho(g) \circ X
\end{aligned} \tag{89}$$

Hence by Schur's lemma we have $X = k \cdot \mathrm{id}_{\mathbb{C}^n}$ for some $k \in \mathbb{C}$. By the normalization of character functions

$$\mathrm{Tr}(X) = \sum_{h\in G} \mathrm{Tr}(\rho(h^{-1}))\mathrm{Tr}(\rho(h)) = |G|, \tag{90}$$

and hence $k = \frac{|G|}{n}$. Equation (88) then gives $\rho \circ \rho^\dagger = \frac{|G|}{n} \mathrm{id}_{\mathrm{Mat}(n)}$ as required. □

# References


[1] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science*, pages 415–425, 2004. IEEE Computer Science Press.

[2] Samson Abramsky and Bob Coecke. *Handbook of Quantum Logic and Quantum Structures*, volume 2, chapter Categorical Quantum Mechanics. Elsevier, 2008.

[3] John C Baez and Mike Stay. *New Structures for Physics*, chapter Physics, Topology, Logic and Computation: A Rosetta Stone, pages 95–172. Springer, 2010.

[4] T. Ceccherini-Silberstein, F. Scarabotti, and F. Tolli. Clifford theory and applications. *Journal of Mathematical Sciences*, 156(1):29–43, 2009.

[5] Dong Pyo Chi and Jinsoo Kim. Quantum database search by a single query. *Lecture Notes in Computer Science*, 1509:148–151, 1999.

[6] Bob Coecke. The logic of entanglement: An invitation. Technical report, University of Oxford, 2003. Computing Laboratory Research Report PRG-RR-03-12.

[7] Bob Coecke and Ross Duncan. Interacting quantum observables: Categorical algebra and diagrammatics. *New Journal of Physics*, 13, 2011.

[8] Bob Coecke and Eric Oliver Paquette. POVMs and Naimark's theorem without sums. 2006.

[9] Bob Coecke, Eric Oliver Paquette, and Dusko Pavlovic. Classical and quantum structuralism. In Simon Gay and Ian Mackie, editors, *Semantic Techniques in Quantum Computation*, pages 29–69. Cambridge University Press, 2010.

[10] Bob Coecke and Dusko Pavlovic. *The Mathematics of Quantum Computation and Technology*, chapter Quantum Measurements Without Sums. Taylor and Francis, 2006.

[11] Bob Coecke, Dusko Pavlovic, and Jamie Vicary. Commutative dagger-Frobenius algebras in FdHilb are orthogonal bases. (RR-08-03), 2008. Technical Report.

[12] Bob Coecke and Simon Perdrix. Environment and classical channels in categorical quantum mechanics. In *Proceedings of the 19th EACSL Annual Conference on Computer Science Logic*, number 6247 in Lecture Notes in Computer Science, 2010.

[13] Sean Hallgren, Alexander Russell, and Amnon Ta-shma. Normal subgroup reconstruction and quantum computation using group representations. In *Proceedings of the 32nd ACM Symposium on Theory of Computing*, 2000.

[14] Peter Høyer. Conjugated operators in quantum algorithms. *Physical Review A*, 59:3280–3289, 1999.

[15] Gregory M. Kelly and Miguel L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[16] Joachim Kock. *Frobenius Algebras and 2D Topological Quantum Field Theories.* Cambridge University Press, 2004.

[17] Samuel Lomonaco and Louis Kauffman. *The Mathematics of Quantum Computation and Quantum Technology*, chapter Quantum Hidden Subgroup Algorithms: An Algorithmic Toolkit, pages 3–46. Chapman & Hall, 2007.

[18] Andrew J. Duncan Michael Batty and Samuel L. Braunstein. Extending the promise of the Deutsch-Jozsa-Høyer algorithm for finite groups. *Journal of Computation and Mathematics*, 9:40–63, 2006.

[19] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[20] Roger Penrose. Applications of negative-dimensional tensors. In D. J. A. Welsh, editor, *Combinatorial Mathematics and its Applications*. Academic Press, 1971.

[21] R. Rosebrugh, N. Sabadini, and R. F. C. Walters. Generic commutative separable algebras and cospans of graphs. *Theory and Applications of Categories*, 15(164–177):6, 2005.

[22] Peter Selinger. *New Structures for Physics*, chapter A Survey of Graphical Languages for Monoidal Categories, pages 289–355. Number 813 in Lecture Notes in Physics. Springer, 2011.

[23] Daniel Simon. On the power of quantum computation. *Foundations of Computer Science*, pages 116–123, 1994.

[24] Jamie Vicary. Higher quantum theory. 2012.